

N. Senthamilarasi, V. Subapriya, Nikitha

Malware Analysis

Author :	N. Senthamilarasi, V. Subapriya, Nikitha
ISBN 13 :	978-93-55389-84-8
ISBN 10 :	9355389841
E-ISBN 13 :	978-93-55389-84-8
Edition :	First
Pages :	132
Type of book :	Physical
Year :	2026
Language :	English
Publisher :	Khanna Publishing House
M.R.P :	Rs 248.00
Categories :	New Arrivals, Emerging Technologies, Book Store, Sathyabama Series
Condition Type :	New
Country Origin :	India

Khanna Publishing House

4C/4344, Ansari Road, Daryaganj, New Delhi-110002

Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320

Product Description

In today's interconnected digital landscape, the threat from malicious software is a constant and rapidly evolving challenge, capable of inflicting significant harm on individuals and organizations. MALWARE ANALYSIS is an essential guide crafted to provide a comprehensive foundation for cybersecurity specialization in both malware analysis and Operating System (OS) security. It is designed to equip students, security professionals, IT professionals, and researchers with the crucial tools and knowledge needed to identify, understand, and effectively neutralize threats in real-world environments.

The book's core value lies in its pragmatic approach, meticulously combining theoretical foundations with indispensable hands-on analysis techniques. Readers will gain an in-depth exploration of both static malware analysis (examining code without execution) and dynamic malware analysis (studying behavior during execution). The content systematically progresses from fundamental concepts of malware types—such as worms, ransomware, and rootkits—and their evolution to advanced analysis techniques. Key topics include setting up an isolated malware analysis lab, using powerful behavioral monitoring tools like Process Monitor and Wireshark, and advanced code-level debugging with tools like OLLYDBG. Furthermore, it covers advanced malware functionality like Process Injection and modern detection techniques, including signature-based, non-signature-based, and machine-learning methods. This text is an indispensable resource for mastering the skills required to safeguard digital infrastructure against emerging and complex cyber threats.

In today's interconnected digital landscape, the threat from malicious software is a constant and rapidly evolving challenge, capable of inflicting significant harm on individuals and organizations. MALWARE ANALYSIS is an essential guide crafted to provide a comprehensive foundation for cybersecurity specialization in both malware

analysis and Operating System (OS) security. It is designed to equip students, security professionals, IT professionals, and researchers with the crucial tools and knowledge needed to identify, understand, and effectively neutralize threats in real-world environments.

The book's core value lies in its pragmatic approach, meticulously combining theoretical foundations with indispensable hands-on analysis techniques. Readers will gain an in-depth exploration of both static malware analysis (examining code without execution) and dynamic malware analysis (studying behavior during execution). The content systematically progresses from fundamental concepts of malware types—such as worms, ransomware, and rootkits—and their evolution to advanced analysis techniques. Key topics include setting up an isolated malware analysis lab, using powerful behavioral monitoring tools like Process Monitor and Wireshark, and advanced code-level debugging with tools like OLLYDBG. Furthermore, it covers advanced malware functionality like Process Injection and modern detection techniques, including signature-based, non-signature-based, and machine-learning methods. This text is an indispensable resource for mastering the skills required to safeguard digital infrastructure against emerging and complex cyber threats.

Salient Features:

● Malware Taxonomy Deep Dive: Explores the fundamental concepts, history, and taxonomy of malicious software, including worms, ransomware, rootkits, spyware, and sophisticated Advanced Persistent Threats (APTs).

● Static Analysis Mastery: Provides thorough instruction on static analysis techniques, covering X86 architecture, the Portable Executable (PE) File Format, and essential concepts like Opcodes and Disassembly for code inspection.

● Dynamic Behavior Profiling: Details the principles of dynamic analysis, including setting up an isolated Malware Sandbox and utilizing key tools like Process Monitor and

Khanna Publishing House
4C/4344, Ansari Road, Daryaganj, New Delhi-110002
Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320

Wireshark to observe runtime behavior and network traffic.

● Practical Lab Setup: Guides the reader through assembling a complete malware analysis toolkit, covering virtualization, isolation techniques, and the use of behavioral monitoring and code-analysis utilities.

● Advanced Debugging Techniques: Teaches practical skills in advanced code-level analysis, including kernel vs. user-mode debugging, setting Breakpoints and Tracing execution, and using debuggers like OLLYDBG.

● Covert Malware Functionality: Discusses sophisticated attack vectors and persistence mechanisms, such as Process Injection, Privilege Escalation, Downloaders, and Credential Stealers.

● Detection & Evasion Tactics: Explores contemporary techniques like signature-based, similarity-based, and Machine Learning methods for detection, alongside malware evasion tactics such as Polymorphic and Metamorphic code.

● Integrated OS Security: Provides fundamental context by linking malware analysis directly to OS Security concepts, including principles like integrity, confidentiality, and availability, and various system threats.

● Malware Taxonomy Deep Dive: Explores the fundamental concepts, history, and taxonomy of malicious software, including worms, ransomware, rootkits, spyware, and sophisticated Advanced Persistent Threats (APTs).

● Static Analysis Mastery: Provides thorough instruction on static analysis techniques, covering X86 architecture, the Portable Executable (PE) File Format, and essential concepts like Opcodes and Disassembly for code inspection.

● Dynamic Behavior Profiling: Details the principles of dynamic analysis, including setting up an isolated Malware Sandbox and utilizing key tools like Process Monitor and Wireshark to observe runtime behavior and network traffic.

Khanna Publishing House

4C/4344, Ansari Road, Daryaganj, New Delhi-110002

Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320

● Practical Lab Setup: Guides the reader through assembling a complete malware analysis toolkit, covering virtualization, isolation techniques, and the use of behavioral monitoring and code-analysis utilities.

● Advanced Debugging Techniques: Teaches practical skills in advanced code-level analysis, including kernel vs. user-mode debugging, setting Breakpoints and Tracing execution, and using debuggers like OLLYDBG.

● Covert Malware Functionality: Discusses sophisticated attack vectors and persistence mechanisms, such as Process Injection, Privilege Escalation, Downloaders, and Credential Stealers.

● Detection & Evasion Tactics: Explores contemporary techniques like signature-based, similarity-based, and Machine Learning methods for detection, alongside malware evasion tactics such as Polymorphic and Metamorphic code.

● Integrated OS Security: Provides fundamental context by linking malware analysis directly to OS Security concepts, including principles like integrity, confidentiality, and availability, and various system threats.

Khanna Publishing House

4C/4344, Ansari Road, Daryaganj, New Delhi-110002

Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320

Author

N. Senthamilarasi

N. Senthamilarasi Associate Professor, Dept of CSE, Sathyabhama Institute of Science and Technology

V. Subapriya

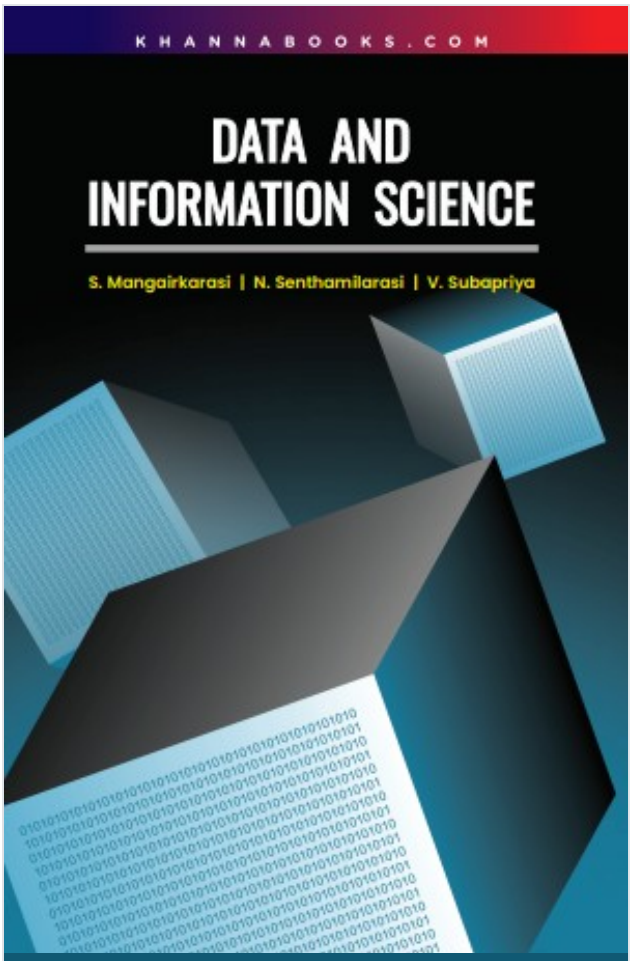
V. Subapriya Associate Professor, Dept of CSE, Sathyabhama Institute of Science and Technology

Nikitha

Khanna Publishing House

4C/4344, Ansari Road, Daryaganj, New Delhi-110002

Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320



S. Mangairkarasi, N. Senthamilarasi, V. Subapriya

Data and Information Science

Author :	S. Mangairkarasi, N. Senthamilarasi, V. Subapriya
ISBN 13 :	978-93-55389-72-5
ISBN 10 :	9355389728
E-ISBN 13 :	978-93-55389-72-5
Edition :	First
Pages :	164
Type of book :	Physical
Year :	2026
Language :	English
Publisher :	Khanna Publishing House
M.R.P :	Rs 298.00
Categories :	New Arrivals, Book Store, Sathyabama Series
Condition Type :	New
Country Origin :	India

Product Description

Data and Information Science

This book provides a comprehensive and practical guide to the multidisciplinary fields of data science and information science. In an increasingly data-driven world, the text addresses the critical need to understand, manage, and extract actionable value from massive data sets in sectors ranging from business to government. It is an essential resource for students, professionals, and hobbyists seeking to master the techniques of this transformative domain. The book systematically explores the entire data lifecycle, from initial data acquisition, preprocessing, and cleaning to advanced subjects like Artificial Intelligence, Big Data Analytics, and Data Ethics.

It successfully bridges the gap between theoretical concepts and practical application by detailing key methodologies, essential tools of Business Intelligence (BI), and providing real-world insights. Readers will gain an in-depth understanding of how to combine computer science, statistics, and machine learning principles to detect patterns, predict outcomes, and drive superior decision-making. Ultimately, this material is designed to equip you with the critical skills needed to utilize data effectively, spur creativity, and confidently participate in the ongoing data-driven revolution.

Salient Features:

- **Full Data Lifecycle**: Presents a complete framework covering all steps of the data lifecycle, from acquisition sources (Web APIs, Relational Databases) to data processing and final analysis.
- **Practical Tool Focus**: Integrates practical tools and libraries like Pandas, NumPy, and Matplotlib for real-world data preparation and implementation in Machine Learning models.

Khanna Publishing House
4C/4344, Ansari Road, Daryaganj, New Delhi-110002
Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320

- **Data Quality Mastery**: Offers detailed strategies for improving data quality, including Data Wrangling, handling missing values, and utilizing Binning, Regression, and Clustering for noisy data.
- **Big Data Principles**: Introduces the fundamental concepts and challenges of Big Data (Volume, Variety, Velocity) and discusses effective strategies for processing and utilizing massive datasets.
- **Text Analysis Techniques**: Dedicated coverage of text-based data handling, exploring methods such as Bag of Words, Regular Expressions, and the practical application of Sentiment Analysis.
- **Visualization and BI**: Provides essential skills in data visualization basics, including creating compelling charts and dashboards using the leading Business Intelligence tool, Tableau.
- **Data Transformation Depth**: Explores the nuances of data transformation, detailing structural changes, normalization, discretization, and the difference between ETL and ELT processes.
- **Open Data Resources:** Highlights key sources for obtaining data, including internal/external systems, Cloud Data Warehouses, and open-source repositories like Kaggle and the UCI Machine Learning Repository.

Khanna Publishing House

4C/4344, Ansari Road, Daryaganj, New Delhi-110002

Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320

Table Of Contents

- Data Acquisition
- Data Processing and Preparation
- Data Quality and Transformation
- Handling Text Data
- Business Intelligence Strategy and Road Map

Author

S. Mangairkarasi

S. Mangairkarasi Associate Professor, Dept of CSE, Sathyabhama Institute of Science and Technology

N. Senthamilarasi

N. Senthamilarasi Associate Professor, Dept of CSE, Sathyabhama Institute of Science and Technology

V. Subapriya

V. Subapriya Associate Professor, Dept of CSE, Sathyabhama Institute of Science and Technology

Khanna Publishing House

4C/4344, Ansari Road, Daryaganj, New Delhi-110002

Email: contact@khannabooks.com | Tel: 011-2324 44 47 - 48 | Mobile: +91-99109 09320